(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－131949
（Ｐ２００３－１３１９４９Ａ）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
G06F 12/14	320	G06F 12/14	320 B	5B017
12/00	537	12/00	537 H	5B082
G09C 1/00	660	G09C 1/00	660 D	5J104

審査請求　未請求　請求項の数５　ＯＬ　（全19頁）

(21)出願番号　特願2001－327302(Ｐ2001－327302)

(22)出願日　平成13年10月25日(2001.10.25)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　安孫子　幸弘
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

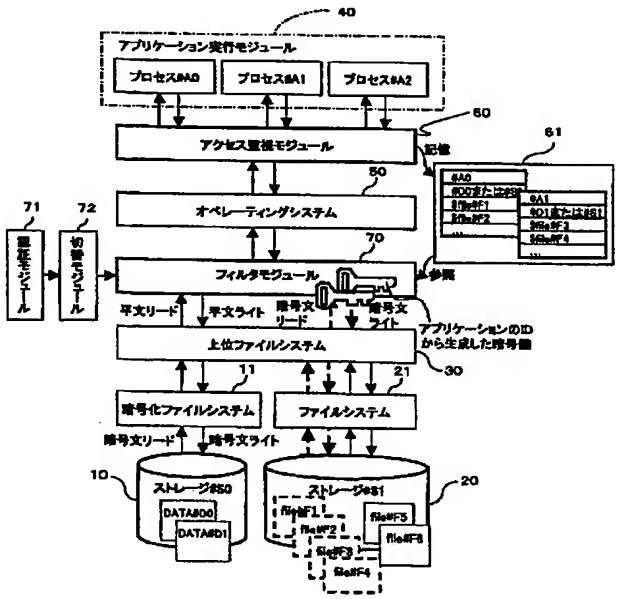
(72)発明者　岡田　佳之
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100092978
弁理士　真田　有

最終頁に続く

(54)【発明の名称】データ管理システム

(57)【要約】
【課題】暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況であっても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護できるようにする。
【解決手段】コンテンツを蓄積する蓄積媒体１０，２０と、アプリケーション実行手段４０と、このアプリケーション実行手段で動作中のアプリケーションの固有情報とアプリケーションがアクセスしているコンテンツの固有情報とを対応付けてアクセス状況を監視するアクセス監視手段６０と、動作中のアプリケーションがコンテンツを蓄積媒体２０に書き込む際にはアプリケーションの固有情報を用いてコンテンツを暗号化する一方、動作中のアプリケーションがコンテンツを蓄積媒体２０から読み出す際にはアプリケーションの固有情報を用いてコンテンツを復号化するフィルタリング手段７０とをそなえて構成する。



1

【特許請求の範囲】

【請求項１】　コンテンツを蓄積する蓄積媒体と、

該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、

該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、

動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ管理システム。

【請求項２】　該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、

該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いることを特徴とする、請求項１記載のデータ管理システム。

【請求項３】　該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視することを特徴とする、請求項１または請求項２に記載のデータ管理システム。

【請求項４】　該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、

該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、

該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、請求項３記載のデータ管理システム。

【請求項５】　該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、

該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、

該ファイルシステムのうちの少なくとも一つが、そのファイルシステムの全体を暗号化した上で該コンテンツを

2

該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、請求項３記載のデータ管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、ハードディスクレコーダ等の記録再生装置やパーソナルコンピュータ等のデータ処理装置を含んで構成されるシステムにおいて、各種ディジタルコンテンツの著作権を保護するための技術に関する。

【０００２】

【従来の技術】近年、ディジタル化技術の発展とストレージ装置の大容量化、そしてネットワークの広帯域化に伴い、映像データ（動画データ）や音声データあるいは画像データなどを含むコンテンツは、ディジタル化後にストレージ装置や可換媒体などの各種記録媒体に蓄積され、ネットワークや可換媒体を介して容易に交換されるようになりつつある。

【０００３】しかし、データの交換が容易になることによって、ユーザは、無意識のうちにあるいは故意に、コンテンツの著作者の許諾なしにデータを配布したり譲渡したりして、著作権を侵害してしまうケースが増加している。そこで、これまでに著作権を保護すべく、著作物を暗号化する技術が開発されてきている。このような技術を導入すると、暗号鍵を入手できない限り、暗号化されたデータ（以下、暗号化データという）は意味をなさないため、暗号化は著作権保護に有効である。

【０００４】ところが、暗号化データをアプリケーションが利用するためには、その暗号化データを復号化して記録媒体に蓄積する必要がある。このように復号化されたデータが、一旦、記録媒体に蓄積された後は、データの移動，複写，改竄などの処理を自由に行なえるようになってしまうので、著作権保護機能が働かなくなることが懸念される。

【０００５】このような状況に対応すべく、従来、例えば特開２０００－３１１１１４号公報や特開２０００－３３０８７０号公報などに開示されるような技術が提案されている。これらの公報に開示された技術では、可換媒体を用いる場合、データを暗号化する際に、媒体固有のメディアＩＤ（IDentification）が暗号鍵として用いられる。メディアＩＤを持たない媒体に対しては、ファイルシステムから通常アクセスできないリードイン領域，交替処理領域，ＲＯＭ（Read Only Memory）領域に書かれる暗号鍵が用いられる。また、ハードディスク装置のように通常特別なＲＯＭ領域を持たない媒体に対しては、ＢＩＯＳ（Basic Input Output System）によって隠蔽されたデバイスＩＤが暗号鍵として用いられる。上述した公報に開示された技術では、これらの暗号鍵によって暗号化されたデータを各媒体に蓄積することによって、著作権が保護されている。

【０００６】
【発明が解決しようとする課題】ところで、既に著作権保護機能なしに運用されているパーソナルコンピュータやデータ記録再生装置などのシステムに、暗号化された著作物（コンテンツ）を含む蓄積媒体を後付けして使用した場合などには、暗号化機能なしの蓄積媒体（暗号化する必要のないデータを蓄積するハードディスク）と暗号化機能ありの蓄積媒体（暗号化データを蓄積するハードディスク）とを混在させて使用する状況が発生する。
【０００７】このような状況下において、アプリケーションが暗号化データを読み出して使用すると、暗号化が解除された著作物データの全部もしくは一部が流通されてしまうことになる。上述した従来技術では、このような状況での著作権保護対策は何ら開示されていない。
【０００８】例えば、編集アプリケーションを利用してデータに変更を加える場合に、中間処理結果をファイルに一時的に保存したりメモリファイルに一時的に蓄積したりする状況を想定する。すると、著作物として意味のある内容を持つ一時蓄積ファイルが、暗号化の対象としている媒体以外において生成され、暗号化されていないデータとして保存されることになる。従って、既存のファイルシステムを用いて、著作権を保護するためのシステムを構築しようとすると、ハードディスク内のデータを全て暗号化する変換作業が求められることになる。しかし、このようなシステムを構築すると、著作者あるいは著作者から許諾を受けている者に対して、著作権の行使が著しく制限されてしまうため、逆に著作権が侵害されてしまう。
【０００９】本発明は、このような課題に鑑み創案されたもので、暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況であっても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護できるようにすることを目的とする。
【００１０】
【課題を解決するための手段】上記目的を達成するために、本発明のデータ管理システム（請求項１）は、コンテンツを蓄積する蓄積媒体と、該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴としている。
【００１１】なお、該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いるように構成してもよい（請求項２）。
【００１２】また、該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視するように構成してもよい（請求項３）。
【００１３】このとき、該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステム（請求項４）、もしくは、そのファイルシステムの全体を暗号化した上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステム（請求項５）であってもよい。
【００１４】
【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。
〔１〕第１実施形態の説明
図１は本発明の第１実施形態としてのデータ管理システムの構成を示すブロック図であり、この図１に示すように、第１実施形態のデータ管理システムは、例えば汎用のパーソナルコンピュータ（データ処理装置）に組み込まれたもので、ストレージ１０，暗号化ファイルシステム１１，ストレージ２０，ファイルシステム２１，上位ファイルシステム３０，アプリケーション実行モジュール４０，オペレーティングシステム５０，アクセス監視モジュール６０，フィルタモジュール７０，認証モジュール７１および切替モジュール７２をそなえて構成されている。
【００１５】第１実施形態のデータ管理システムには、２つのストレージ１０および２０がそなえられており、各ストレージ１０，２０に一つの論理ドライブが構築されている。なお、図１に示す例では、ストレージ１０，２０にそれぞれ構築された論理ドライブのドライブ名を＃Ｓ０，＃Ｓ１としている。
【００１６】ストレージ１０は、後述する暗号化ファイルシステム１１で管理される論理ドライブを含む第１蓄積装置（暗号化機能ありの蓄積媒体）として機能するも

のである。暗号化ファイルシステム１１は、コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有しファイル毎またはフォルダ毎に暗号化を行なった上でコンテンツ（著作物ファイル）をストレージ１０に蓄積させるもの、もしくは、そのファイルシステムの全体を暗号化した上でコンテンツ（著作物ファイル）をストレージ１０に蓄積させるものである。

【００１７】従って、ストレージ１０の論理ドライブにデータを書き込むと、そのデータは、暗号化ファイルシステム１１によって暗号化されてから書き込まれる一方、ストレージ１０の論理ドライブから暗号化データを読み出すと、その暗号化データは、暗号化ファイルシステム１１によって復号化されてから読み出されるようになっている。なお、図１では、ストレージ１０に、暗号化された２つの著作物ファイル（ファイル名＃Ｄ０，＃Ｄ１）を蓄積した例が示されている。

【００１８】ストレージ２０は、後述するフィルタモジュール７０によって暗号化されたコンテンツを蓄積する第２蓄積装置（暗号化機能なしの蓄積媒体）として機能するものである。このストレージ２０に構築された論理ドライブは、例えばＦＡＴ（File Allocation Table）等のファイルシステム２１によって管理されている。なお、図１では、ストレージ２０に、暗号化された４つのファイル（ファイル名＃Ｆ１～＃Ｆ４）と暗号化されていない２つのファイル（ファイル名＃Ｆ５，＃Ｆ６）とを蓄積した例が示されている。

【００１９】上位ファイルシステム３０は、暗号化ファイルシステム１１およびファイルシステム２１の両方を管理するもので、これらのファイルシステム１１，１２と後述するフィルタモジュール７０との間に介在するものである。アプリケーション実行モジュール（アプリケーション実行手段）４０は、ストレージ１０，２０におけるコンテンツにアクセスし、そのコンテンツに対する処理を行なうアプリケーションを動作させるものである。

【００２０】オペレーティングシステム５０は、アプリケーションの実行を制御するソフトウェアである。本実施形態のオペレーティングシステム５０は、マルチプロセスに対応可能なものであり、アプリケーション実行モジュール４０がアプリケーションを実行する際にプロセス毎に識別情報（プロセスＩＤ）を付与し、そのプロセスＩＤを用いてアプリケーションを呼び出したり、アプリケーションがファイルシステム１１，２１を呼び出すときにストレージ１０，２０に応じた適切なファイルシステム１１，２１のＡＰＩ（Application Programming Interface）を呼び出したりするものである。

【００２１】なお、図１では、ストレージ１０の著作物ファイルにアクセスして動作しているアプリケーションによる２つのプロセスに対し、それぞれ、プロセスＩＤとして＃Ａ０，＃Ａ１を付与し、ストレージ１０の著作物ファイルにアクセスせずに動作しているアプリケーションによるプロセスに対し、プロセスＩＤとして＃Ａ２を付与した例が示されている。これらのプロセス＃Ａ０～＃Ａ２は、同一のアプリケーションによって実行されるものであっても、それぞれ異なるアプリケーションによって実行されるものであってもよい。

【００２２】また、アプリケーションは、汎用のパーソナルコンピュータ上で動作するもので、本発明のデータ管理システム専用のものであることは特に要求されない。例えば編集ソフトウェアやＷｅｂブラウザがこれにあたる。アプリケーション実行モジュール４０でアプリケーションを実行する際には、各アプリケーションの動作は、オペレーティングシステム５０によってプロセスとして管理される。

【００２３】アクセス監視モジュール（アクセス監視手段）６０は、アプリケーション実行モジュール４０で動作中のアプリケーションについての固有情報と各アプリケーション（各プロセス）がアクセスしているコンテンツについての固有情報とを対応付けて管理テーブル（リスト）６１に登録し、この管理テーブル６１を用いて各アプリケーションのコンテンツへのアクセス状況を監視するものである。

【００２４】このとき、本実施形態では、アプリケーションについての固有情報としては、オペレーティングシステム５０からプロセス毎に付与されるプロセスＩＤが用いられ、コンテンツについての固有情報としては、コンテンツを含む著作物ファイルのファイル名、もしくは、その著作物ファイルを含む論理ドライブのドライブ名が用いられる（後述する機能(1)参照）。

【００２５】また、アプリケーション実行モジュール４０がアプリケーション（プロセス）の実行を終了した場合、アクセス監視モジュール６０は、そのアプリケーションについての固有情報（プロセスＩＤ）とこれに対応するコンテンツについての固有情報（ファイル名）とを管理テーブル６１から削除する。

【００２６】つまり、アクセス監視モジュール６０は、アプリケーションのファイルアクセスを監視し、ファイルアクセスを行なったアプリケーション（プロセス）毎にアクセスした著作物ファイルのファイル名の一覧（管理テーブル６１）を作成し、少なくともアプリケーションが終了するまでそのファイル名を記憶しておき、特にオペレーティングシステム５０がアプリケーションにプロセスＩＤを与える場合には、その一覧にアプリケーション（プロセス）の固有情報としてプロセスＩＤを登録して記憶しておく。

【００２７】そして、本実施形態のアクセス監視モジュール６０は、以下のような機能(1)～(5)を有していてもよい。

機能(1)：暗号化ファイルシステム１１で管理されるストレージ１０（論理ドライブ＃Ｓ０）に蓄積された著作

物ファイル（コンテンツ）をアプリケーションが読み出す際に、コンテンツについての固有情報として、アプリケーションが読み出したコンテンツを含む著作物ファイルのファイル名を管理テーブル６１に登録する機能。登録されるファイル名には、アプリケーションが読み出したコンテンツを蓄積する論理ドライブのドライブ名が含まれている。

【００２８】機能(2)：アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルのファイル名を、アプリケーションについての固有情報（プロセスＩＤ）に対応させて、管理テーブル６１に登録する機能。このとき、新たに生成されたファイルのファイル名の一部もしくは全部を変更したものを管理テーブル６１に登録してもよい。ここで用いられるファイル名は、そのファイルが蓄積される論理ドライブのドライブ名を含む文字列であり、そのドライブ名の部分を変更することにより、ファイルの蓄積先媒体（ストレージ１０，２０）を変更したり、そのファイルをメモリファイルとして一次記憶手段（蓄積媒体；図示省略）に一時的に記憶させたりすることができる。また、暗号化ファイルシステム１１（ストレージ１０）から読み出された著作物ファイルのファイル名を、新たに生成されたファイルのファイル名として登録・記憶してもよい。

【００２９】機能(3)：アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル６１に登録された論理ドライブのドライブ名（ファイル名に含まれるドライブ名）とを比較し、その比較結果が不一致である場合、管理テーブル６１に登録されたドライブ名の論理ドライブに新たに生成されたファイルが蓄積されるように、そのファイル名を変更して管理テーブル６１に登録する機能。即ち、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ（著作物ファイル）を蓄積している論理ドライブとが異なる場合、同じ論理ドライブ（同じストレージ１０）に新たなファイルが生成されるようにファイル名を変更して管理テーブル６１に登録する機能。この機能(3)により、新たに生成されたファイルを、元のコンテンツと同じ論理ドライブ（同じストレージ１０）に生成・蓄積することができ、暗号化機能ありのストレージ１０から読み出されたコンテンツに基づいて生成されたファイルは、暗号化ファイルシステム１１により暗号化されてからストレージ１０に書き込まれることになる。

【００３０】機能(4)：アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル６１に登録された論理ドライブのドライブ名（ファイル名に含まれるドライブ名）とを比較し、その比較結果が一致した場合、新たに生成されたファイルのファイル名の、管理テーブル６１への登録を禁止する機能。つまり、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ（著作物ファイル）を蓄積している論理ドライブとが同じ場合、新たに生成されたファイルは、後述のフィルタモジュール７０による暗号化処理を施さなくても、暗号化ファイルシステム１１により暗号化されてからストレージ１０に書き込まれることになる。従って、このような場合、本実施形態では、新たに生成されたファイルのファイル名の、管理テーブル６１への登録を禁止してそのファイル名を登録・記憶しないようにすることにより、フィルタモジュール７０が、無駄な暗号化処理を行なわないようにすることできる。

【００３１】機能(5)：アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル６１に登録された論理ドライブのドライブ名（ファイル名に含まれるドライブ名）とを比較し、その比較結果が不一致である場合、後述するごとくフィルタモジュール７０により新たに生成されたファイルを暗号化してから蓄積先論理ドライブ（ストレージ１１）に蓄積させる機能。つまり、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ（著作物ファイル）を蓄積している論理ドライブとが異なる場合、フィルタモジュール７０の動作を有効化する機能。このとき、上記機能(2)を用い、後述するフィルタモジュール７０が、暗号化した新たに生成されたファイルを、蓄積先論理ドライブに代えて一次記憶手段にメモリファイルとして一時的に蓄積するように、そのファイル名の一部もしくは全部を変更して管理テーブル６１に登録してもよい。

【００３２】上述したアクセス監視モジュール６０の機能を用いて、図１に示す管理テーブル６１には、ストレージ１０の著作物ファイルにアクセスして動作しているアプリケーションによる２つのプロセスの識別情報＃Ａ０，＃Ａ１が登録されている。そして、プロセス＃Ａ０については、このプロセス＃Ａ０によってアクセスされている著作物ファイルのファイル名＃Ｄ０（論理ドライブ名＃Ｓ０を含む）が登録されるとともに、このプロセス＃Ａ０により著作物ファイル＃Ｄ０に基づいて生成・展開された２つの新たなファイルのファイル名$file＃Ｆ１，$file＃Ｆ２が登録されている。同様に、プロセス＃Ａ１については、このプロセス＃Ａ１によってアクセスされている著作物ファイルのファイル名＃Ｄ１（論理ドライブ名＃Ｓ０を含む）が登録されるとともに、このプロセス＃Ａ１により著作物ファイル＃Ｄ１に基づいて生成・展開された２つの新たなファイルのファイル名$file＃Ｆ３，$file＃Ｆ４が登録されている。

【００３３】なお、ファイル$file＃Ｆ１～$file＃Ｆ２は、後述するフィルタモジュール７０により暗号化され、ファイルシステム２１を通じて暗号化機能のないス

トレージ２０に蓄積されている。また、アクセス監視モジュール６０の処理手順については、図２を参照しながら後述する。

【００３４】フィルタモジュール（フィルタリング手段）７０は、アクセス監視モジュール６０で作成した管理テーブル６１を参照し、動作中のアプリケーション（プロセス）が、コンテンツを含むデータを、暗号化機能のないストレージ２０において新たに生成されたファイルに書き込む際には、アプリケーションについての固有情報、即ちプロセスＩＤにより生成された暗号鍵を用いてコンテンツを含むデータ（ファイル）を暗号化するものである。逆に、動作中のアプリケーション（プロセス）が、上述のごとく暗号化されたデータを、暗号化機能のないストレージ２０のファイルから読み出す際には、フィルタモジュール７０は、上述のごとく生成される暗号鍵を用いてデータ（コンテンツ）を復号化するものである。

【００３５】なお、暗号化されたファイルをストレージ間で単に移動する際、フィルタモジュール７０による暗号化処理／復号化処理は実行されない。また、フィルタモジュール７０の処理手順については、図３を参照しながら後述する。さらに、ユーザがパスワードを入力することにより、フィルタモジュール７０による暗号化処理／復号化処理を有効化／無効化して運用上の不都合を解決するため、フィルタモジュール７０には、認証モジュール７１および切替モジュール７２がそなえられている。

【００３６】認証モジュール（認証手段）７１は、ユーザの本人認証を行なうためのもので、ユーザによって入力されたパスワードと予め登録されている当該ユーザのパスワードとを比較し、これらが一致した場合にパスワードを入力したユーザが本人であることを認証するものである。切替モジュール（切替手段）７２は、認証モジュール７１によってユーザの本人認証が行なわれた場合にのみフィルタモジュール７０の動作の有効化／無効化を切り替えるものである。

【００３７】上述したアプリケーション実行モジュール４０，アクセス監視モジュール６０，フィルタモジュール７０，認証モジュール７１および切替モジュール７２は、専用ソフトウェア（データ管理プログラム）によって実現される。このデータ管理プログラムは、例えばフレキシブルディスク，ＣＤ－ＲＯＭ等のコンピュータ読取可能な記録媒体に記録された形態で提供される。本実施形態においては、汎用のパーソナルコンピュータ（データ処理装置）を成すＲＯＭ（Read Only Memory；図示省略）等に予めデータ管理プログラムを格納しておき、このデータ管理プログラムを、やはり汎用のパーソナルコンピュータ（データ処理装置）を成すＣＰＵ（図示省略；コンピュータ）によって読み出し実行することで、上述したアプリケーション実行モジュール４０，アクセス監視モジュール６０，フィルタモジュール７０，認証モジュール７１および切替モジュール７２としての機能が実現される。

【００３８】なお、データ管理プログラムは、例えば磁気ディスク，光ディスク，光磁気ディスク等の記憶装置（記録媒体）に記録しておき、その記憶装置から通信経路を介してコンピュータに提供されてもよい。また、上述したストレージ１０，２０は、汎用のパーソナルコンピュータ（データ処理装置）を成すコンピュータに内蔵されたＲＡＭ（Random Access Memory；図示省略）やハードディスクなどの記憶装置（あるいは外付けの記憶装置）によって実現される。

【００３９】次に、図２および図３を参照しながら、上述のごとく構成された第１実施形態のデータ管理システムの動作について説明する。まず、図２に示すフローチャート（ステップＳ１１～Ｓ２２）に従って、第１実施形態のデータ管理システムにおけるアクセス監視モジュール６０の処理手順について説明する。

【００４０】アクセス監視モジュール６０は、アプリケーションの処理のために復号化された著作物データおよびその一部が、暗号化されずにストレージ２０に保存されることを防止するため、暗号化すべきデータの一覧（管理テーブル６１）を作成する。

【００４１】そのための動作について、図２に示すフローチャートに従って説明すると、アクセス監視モジュール６０は、初期設定を行なった後（ステップＳ１１）、アプリケーション（プロセス）からオペレーティングシステム５０に対する関数の呼出（Call）が行なわれたか否かを判定する（ステップＳ１２）。関数の呼出が行なわれた場合（ステップＳ１２のＹＥＳルート）、呼出（Call）対象の関数がリード関数であるか否かを判定する（ステップＳ１３）。

【００４２】リード関数である場合（ステップＳ１３のＹＥＳルート）、リード対象のファイルの暗号属性を取得してから（ステップＳ１４）、そのファイルが、暗号化されている著作物データ（著作物ファイル）であるか否かを判定する（ステップＳ１５）。著作物データである場合（ステップＳ１５のＹＥＳルート）、管理テーブル６１にアプリケーションの固有情報（オペレーティングシステム５０によって付与されたプロセスＩＤ）と、著作物データのファイル名（論理ドライブ名を含む）とを登録する（ステップＳ１６）。このとき、上述した機能(1)が用いられる。この後、オペレーティングシステム５０に対する関数の呼出（Call）を行ない（ステップＳ１７）、ステップＳ１２に戻る。

【００４３】呼出（Call）対象の関数がリード関数ではない場合（ステップＳ１３のＮＯルート）や、リード対象のファイルが、著作物データではなく、暗号化する必要のないものである場合（ステップＳ１５のＮＯルート）には、直ちにステップＳ１７へ移行する。

【００４４】一方、アプリケーション（プロセス）からオペレーティングシステム５０に対する関数の呼出が行なわれなかった場合（ステップＳ１２のＮＯルート）には、オペレーティングシステム５０から登録対象アプリケーションへのオープン関数のリターンが行なわれ、且つ、ファイルのオープンに成功しているか否かを判定する（ステップＳ１８）。

【００４５】オープン関数のリターンが行なわれ、且つ、ファイルのオープンに成功している場合（ステップＳ１８のＹＥＳルート）、そのファイルの保存先論理ドライブ（蓄積先論理ドライブ）のドライブ名を取得してから（ステップＳ１９）、そのドライブ名が、管理テーブル６１に登録されている著作物データ（著作物ファイル）の蓄積先論理ドライブのドライブ名と同じか否か、つまり、そのファイルの蓄積先論理ドライブと著作物データの蓄積先論理ドライブとが同一か否かを判定する（ステップＳ２０）。

【００４６】同一ではないと判定された場合（ステップＳ２０のＮＯルート）、管理テーブル６１において、登録対象アプリケーションの固有情報（オペレーティングシステム５０によって付与されたプロセスＩＤ）に対応付けて、オープンされたファイルのファイル名を登録する（ステップＳ２１）。このとき、上述した機能(2)や機能(5)が用いられる。この後、登録対象アプリケーションに対するオープン関数のリターンを行なった後（ステップＳ２２）、ステップＳ１２に戻る。

【００４７】オープン関数のリターンが行なわれなかった場合やファイルのオープンに失敗している場合（ステップＳ１８のＮＯルート）には、直ちにステップＳ２２へ移行する。また、ファイルの蓄積先論理ドライブと著作物データの蓄積先論理ドライブとが同一であると判定された場合（ステップＳ２０のＹＥＳルート）にも、後述する理由により、ステップＳ２１による登録を行なうことなく、直ちにステップＳ２２へ移行する。このとき、上述した機能(4)が用いられる。なお、ステップＳ２１では、機能(2)に代えて、上述した機能(3)を用いてもよい。

【００４８】ここで、アクセス監視モジュール６０の動作をより具体的に説明する。まず、アクセス監視モジュール６０は、アプリケーション（プロセス）のファイルアクセスを監視して、著作物データにアクセスしたアプリケーションに対して、アプリケーション固有の情報を取得する。例えば、オペレーティングシステム５０のカーネルモジュールのラッパーモジュールによって、アプリケーションのファイルアクセスＡＰＩ呼出しを検出し、呼出し元のアプリケーションのプロセスＩＤを取得する。プロセスＩＤの他にもアプリケーション名や検出時刻などを合わせて取得してもよい。アクセス監視モジュール６０は、さらに著作物データを含むファイルのファイル名を取得する。そして、取得されたアプリケーション固有の情報や著作物データのファイル名は対応付けられて管理テーブル５１に登録される（ステップＳ１６）。ファイル名は、前述した通り、蓄積されている論理ドライブ名を含む文字列である。

【００４９】ステップＳ１５においてリード対象のファイルが著作物データであるか否かを判定する際、そのファイルが保存されている論理ドライブに利用されているファイルシステムが暗号化ファイルシステムであることが予め認識されていれば、そのことだけでリード対象のファイルが著作物データとみなしてもよく、暗号化ファイルシステムがファイルやフォルダに対して暗号属性を設定するものである場合には、この暗号属性を利用して著作物データの判定を行なう。

【００５０】また、アクセス監視モジュール６０は、ステップＳ１５において上述のように著作物データであるか否かを判定する際、ファイルシステムから得られる情報だけでなく、Ｗｅｂブラウザやストリーミング映像再生アプリケーションなどで行なわれるようにサーバ接続時の認証手続きをフックしてもよい。ストリーミング映像再生アプリケーションは再生処理のためにストレージに中間ファイルを生成することがある。特に、ストリーミングにおける著作権保護では、ダウンロードと異なり、ストレージに蓄積しないことが前提となっているので、上述のようにストリーミング映像サーバとの認証手続きをフックすることによって、この中間ファイルに対しても後述の暗号化処理を適用することが可能となる。

【００５１】一方、アクセス監視モジュール６０は、登録対象アプリケーションが新たにファイルを生成する際にそのファイル名を取得し、暗号化対象ファイルとして管理テーブル６１に登録する。暗号化対象ファイルが登録対象アプリケーションによってアクセスされた著作物データと同じ論理ドライブに蓄積される場合（ステップＳ２０のＹＥＳルート）には、次の考え方から、管理テーブル６１に対する登録を行なう必要がない。

【００５２】一つ目の考え方は、著作物データが蓄積されている論理ドライブ（ストレージ１０）であれば、暗号化対象ファイルは、自動的に、暗号化ファイルシステム１１によって暗号化されて、その論理ドライブに蓄積されるためである。二つ目の考え方は、著作物データが蓄積されている論理ドライブ（ストレージ１０）であれば、データが外部へ流出することがないためである。

【００５３】逆に、これらの考え方から、ステップＳ２１において上述した機能(3)を用いて、暗号化対象ファイルのファイル名の一部を変更することにより、著作物データが蓄積されている論理ドライブに暗号化対象ファイルが蓄積されるようにすることも有効である。例えば、アプリケーションからの暗号化対象ファイルへのアクセスをフックし、ファイル名の論理ドライブ名をあらわす文字列を、著作物データが蓄積されている論理ドライブのドライブ名に置き換えるような変更を行なう。こ

れは、著作物データと異なる論理ドライブへのファイルの書き込みを禁止する場合に有効である。

【００５４】アクセス監視モジュール６０は、アプリケーション実行モジュール４０で登録対象アプリケーションが動作を終了する際に、管理テーブル６１からそのアプリケーションに関するデータを全て消去する。つまり、アプリケーション固有の情報，著作物データのファイル名，暗号化対象ファイル名などが管理テーブル６１から除かれる。

【００５５】ついで、図３に示すフローチャート（ステップＳ３１～Ｓ４５）に従って、第１実施形態のデータ管理システムにおけるフィルタモジュール７０の処理手順について説明する。フィルタモジュール７０は、アプリケーションからのファイルアクセスに応じて、管理テーブル６１を参照して暗号化／復号化を行なう。

【００５６】その動作について、図３に示すフローチャートに従って説明すると、フィルタモジュール７０は、初期設定を行なった後（ステップＳ３１）、ファイルシステム関数の呼出（Call）が行なわれたか、もしくは、ファイルシステム関数からの復帰（Return）が行なわれたかを判定する（ステップＳ３２）。ファイルシステム関数の呼出が行なわれた場合（ステップＳ３２のＹＥＳルート）、ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール７２で有効化されているか否かを判定する（ステップＳ３３）。

【００５７】ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール７２により有効化されている場合（ステップＳ３３のＹＥＳルート）、そのファイルに対するアクセスがライトアクセスであるか否かを判定する（ステップＳ３４）。ファイルへのアクセスがライトアクセスである場合（ステップＳ３４のＹＥＳルート）、管理テーブル６１を参照してアプリケーションの固有情報（プロセスＩＤ）を取得し、そのプロセスＩＤから暗号鍵を生成し（ステップＳ３５）、その暗号鍵を用いてライト対象のデータを暗号化する（ステップＳ３６）。この後、処理をファイルシステムに渡し（ファイルシステム関数ＣＡＬＬ；ステップＳ３７）、ステップＳ３２に戻る。

【００５８】ファイルへのアクセスがライトアクセスではない場合（ステップＳ３４のＮＯルート）、そのアクセスがリードアクセスであるか否かを判定する（ステップＳ３８）。ファイルへのアクセスがリードアクセスである場合（ステップＳ３８のＹＥＳルート）、管理テーブル６１を参照してファイル名変更が必要であるか否かを判定する（ステップＳ３９）。

【００５９】ファイル名変更が必要である場合（ステップＳ３９のＹＥＳルート）、そのファイル名を変更する（ステップＳ４０）。この後、処理をファイルシステムに渡し（ステップＳ３７）、ステップＳ３２に戻る。ファイルが暗号化対象でない場合や暗号化機能が切替モジュール７２により有効化されていない場合（ステップＳ３３のＮＯルート）、あるいは、暗号化対象ファイルへのアクセスがリードアクセスでない場合（ステップＳ３８のＮＯルート）、あるいは、そのファイルへのファイル名変更が必要でない場合（ステップＳ３９のＮＯルート）、直ちにステップＳ３７へ移行する。

【００６０】一方、ファイルシステム関数からの復帰（Return）の場合（ステップＳ３２のＮＯルート）、ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール７２で有効化されているか否かを判定する（ステップＳ４１）。ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール７２により有効化されている場合（ステップＳ４１のＹＥＳルート）、そのファイルに対するアクセスがリードアクセスであるか否かを判定する（ステップＳ４２）。

【００６１】ファイルへのアクセスがリードアクセスである場合（ステップＳ４２のＹＥＳルート）、管理テーブル６１を参照してアプリケーションの固有情報（プロセスＩＤ）を取得し、そのプロセスＩＤから暗号鍵を生成し（ステップＳ４３）、その暗号鍵を用いてリード対象のデータを復号化する（ステップＳ４４）。この後、処理をファイルシステム関数の呼出元に渡し（RETURN；ステップＳ４５）、ステップＳ３２に戻る。

【００６２】ファイルが暗号化対象でない場合や暗号化機能が切替モジュール７２により有効化されていない場合（ステップＳ４１のＮＯルート）、あるいは、暗号化対象ファイルへのアクセスがリードアクセスでない場合（ステップＳ４２のＮＯルート）、直ちにステップＳ４５へ移行する。

【００６３】ここで、フィルタモジュール７０の動作をより具体的に説明する。上述した通り、暗号鍵は、管理テーブル６１に登録されているアプリケーション固有の情報を用いて生成される。例えば、前述したようにオペレーティングシステム５０によって与えられたプロセスＩＤを利用することが考えられる。

【００６４】プロセスＩＤを暗号鍵として利用して暗号化されたファイルは、他の登録対象アプリケーションからアクセスされたとしても、異なる暗号鍵が使用されることになるので、復号化されない。さらに、同じアプリケーションで同様の手順で暗号化ファイルにアクセスしようとしても、やはりプロセスＩＤが異なるので、暗号鍵を生成してもその暗号化ファイルを復号化することはできない。

【００６５】なお、偶然に同じプロセスＩＤを持つアプリケーションが存在しても、異なる登録対象アプリケーションによる暗号化ファイルの復号化が行なわれることを防ぐにためには、プロセスＩＤとともに時刻情報なども暗号鍵生成に利用することが有効である。例えば、登録対象アプリケーションによる著作物データへのファイルアクセスをアクセス監視モジュール６０が検出した時

刻などを用いる。また、登録対象アプリケーションによるファイル生成をアクセス監視モジュール６０が検出した時刻を用いてもよい。時刻情報を加味することにより同一暗号鍵生成を防ぐことができる理由は、オペレーティングシステム５０が同一のシステム上で同時刻に同じプロセスＩＤを与え得ないからである。

【００６６】暗号鍵は、フィルタモジュール７０内のみに保持され、通信路で伝送されたりストレージ１０，２０に保存されることはないので、暗号鍵の盗難の可能性は低い。しかし、オペレーティングシステムによっては、プロセスＩＤを比較的容易に取得することが可能であるので、より堅牢性を高めるために、上述のアプリケーション固有の情報から擬似乱数を演算したものを作業鍵として用いてもよい。

【００６７】データに対する暗号化アルゴリズムについては、ファイルが、通常、バイト列として扱われるので、ブロック暗号方式が適している。フィルタモジュール７０は、オペレーティングシステム５０からのファイルアクセスをフックして暗号化あるいは復号化を行なう（ステップＳ３４またはＳ４４）。ライトアクセスの場合は、オペレーティングシステム５０を経由して受け取ったデータ（ファイル）を、上述のように暗号化した後、ファイルシステム２１に渡す。リードアクセスの場合は、ファイルシステム２１から受け取った暗号化データを復号化してオペレーティングシステム５０に渡す。

【００６８】なお、暗号化対象ファイルが、管理テーブル６１に登録されている著作物データが蓄積されている論理ドライブ（または蓄積媒体）と同じ論理ドライブ（または蓄積媒体）に生成される場合、ある特定の暗号化ファイルシステム、あるいはファイルやフォルダ毎に暗号属性を設定可能な暗号化ファイルシステムに対しては、暗号化対象ファイルに対してフィルタモジュール７０で暗号化／復号化を行なう必要がない。

【００６９】また、著作者自身や、著作者の許諾を得た者、例えば著作物を編集するなど二次著作物を生成する者に対しては、フィルタモジュール７０の暗号化／復号化処理を無効化する必要がある。そこで、本実施形態では、所定のパスワードによりフィルタモジュール７０の暗号化／復号化処理を無効化できるようになっている。

【００７０】つまり、ユーザが、フィルタモジュール７０の暗号化／復号化処理を無効化もしくは有効化する際には、認証モジュール７１に対してパスワードを入力する。この認証モジュール７１においては、ユーザによって入力されたパスワードと予め登録されている当該ユーザのパスワードとが比較され、これらが一致した場合にパスワードを入力したユーザが本人であると認証される。そして、認証モジュール７１によってユーザの本人認証が行なわれた場合にのみ、切替モジュール７２により、フィルタモジュール７０の動作は有効状態から無効状態に切り替えられる。

【００７１】このように、本発明の第１実施形態としてのデータ管理システムによれば、暗号機能ありのストレージ１０，２０に蓄積されたコンテンツがアプリケーションによってアクセスされると、そのアクセス状況がアクセス監視モジュール６０によってアプリケーション（プロセス）毎に管理され、アプリケーションによって読み出されて利用されているコンテンツは、そのアプリケーションについての固有情報であるプロセスＩＤを用いフィルタモジュール７０によって暗号化／復号化される。

【００７２】そして、暗号化ファイルシステム１１によってストレージ１０に蓄積された、暗号化された著作物データをアプリケーションが利用する場合、その暗号化データを一旦復号化する必要があるので、このアプリケーションが新たに生成したファイルには、復号化された著作物データが含まれる可能性が高い。そこで、本実施形態では、少なくとも暗号化された著作物データをアプリケーションがアクセスする際、アクセス監視モジュール６０が管理テーブル６１にアプリケーションの固有情報を登録し、さらにアプリケーションが新たに生成しようとするファイルのファイル名も登録しておくことで、アプリケーションが、読み出し元の暗号機能のあるストレージ１０ではない、暗号機能のないストレージ２０に書き込むファイルに対して、フィルタモジュール７０がデータを暗号化することが可能となる。

【００７３】これにより、暗号化機能なしのストレージ２０と暗号化機能ありのストレージ１０とを混在させて使用する状況下において、アプリケーションが、暗号機能ありのストレージ１０に蓄積された暗号化コンテンツ（著作物データ）を読み出し、そのコンテンツを暗号化機能なしのストレージ２０に一時的に新しいファイルとして格納しながら利用したとしても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護することができ、データ管理システムの性能向上に寄与するところが大きい。

【００７４】つまり、ディジタル化された著作物データ（ディジタルコンテンツ）が暗号化された上で暗号機能なしのストレージ２０に蓄積されるので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意にストレージ２０のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【００７５】アプリケーションが読み出し元と同じストレージ１０，２０に新たなファイルを生成してそのファイルにコンテンツを格納する場合、そのコンテンツは、ストレージ１０，２０毎のファイルシステムに従って書き込まれる。つまり、アプリケーションが元々暗号化さ

れていないファイルのコンテンツにアクセスしている間は、暗号化を施すことなくコンテンツが書き込まれる。一方、アプリケーションが、暗号化ファイルシステム１１で管理される論理ドライブから暗号化ファイルを読み出し、読み出し元以外に新たなファイルを生成してそのファイルにコンテンツ（著作物データ）を格納する場合、そのコンテンツ（ファイル）は、アプリケーションの固有情報（プロセスＩＤ）で暗号化されるので、アプリケーションが処理を終了するまでは、そのファイルを生成したアプリケーションのみがそのコンテンツ（ファイル）を復号化して利用することができる。

【００７６】このとき、アプリケーションについての固有情報として、オペレーティングシステム５０によって与えられるプロセスＩＤのような動的な情報を用い、その情報でコンテンツの暗号化を行なうことにより、同じアプリケーションであっても起動時期が異なると復号化することができず、暗号機能なしのストレージ２０上のファイルを通して復号化されたデータが容易に交換されなくなるので、著作権の侵害をより確実に防ぐことができる。

【００７７】また、ユーザの本人認証が行なわれた場合にのみフィルタモジュール７０の動作の有効化／無効化を切り替えることにより、著作者自身や著作者の許諾を得た者（例えば著作物を編集するなど二次著作物を生成する者）を登録しておけば、著作者自身や著作者の許諾を得た者は、フィルタモジュール７０の動作（暗号化／復号化処理）を無効化することができ、作業を不当に制限されず、著作権の行使の著しい制限に伴う著作権侵害の発生を防止することができる。

【００７８】さらに、ストレージ１０（論理ドライブ＃Ｓ０）が、コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有しファイル毎またはフォルダ毎に暗号化を行なった上でコンテンツ（著作物ファイル）をストレージ１０に蓄積させる暗号化ファイルシステム１１、もしくは、そのファイルシステムの全体を暗号化した上でコンテンツ（著作物ファイル）をストレージ１０に蓄積させる暗号化ファイルシステム１１によって管理され、ディジタル化された著作物データが暗号化された上でストレージ１０に蓄積されているので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意にストレージ１０のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【００７９】また、アクセス監視モジュール６０の機能(5)を用いることにより、フィルタモジュール７０が、暗号化した新たに生成されたファイルを、蓄積先論理ドライブに代えて一次記憶手段にメモリファイルとして一時的に蓄積するように、そのファイル名の一部もしくは全部が変更されて管理テーブル６１に登録される。これにより、新たに生成されたファイルは、フィルタモジュール７０によって暗号化された上で一次記憶手段に記憶されるので、一旦、電源が切られると、一次記憶手段に蓄積された暗号化ファイルは、消去され、一次記憶手段に保持され続けることがないので、より確実に著作権が侵害されるのを防ぐことができる。

【００８０】〔１－１〕第１実施形態の変形例の説明

図４は第１実施形態のデータ管理システムの変形例の構成を示すブロック図であり、この図４において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その説明は省略する。

【００８１】図１に示す第１実施形態のデータ管理システムでは、２つのストレージ１０および２０をそなえ、各ストレージ１０，２０に一つの論理ドライブ＃Ｓ０，＃Ｓ１が構築されている場合について説明したが、図４に示すごとく、２つのストレージ１０，２０に代えて一つのストレージ（蓄積媒体）８０をそなえ、このストレージ８０を複数（図４では２つ）のパーティションに分け、これらのパーティションをそれぞれ論理ドライブ＃Ｐ０，＃Ｐ１として用いてもよい。

【００８２】ここで、論理ドライブ＃Ｐ０は、暗号化ファイルシステム１１によって管理され暗号化機能ありの蓄積媒体（図１の論理ドライブ＃Ｓ０に対応）として機能するとともに、ファイルシステム２１によって管理され論理ドライブ＃Ｐ１は、暗号化機能なしの蓄積媒体（図１の論理ドライブ＃Ｓ１に対応）として機能する。この場合も、本発明は、上述した第１実施形態と同様に適用され、上述した第１実施形態と同様の作用効果を得ることができる。

【００８３】〔２〕第２実施形態の説明

図５は本発明の第２実施形態としてのデータ管理システムの構成を示すブロック図であり、この図５に示すように、第２実施形態のデータ管理システムも第１実施形態のものと同様に構成されているが、第２実施形態のデータ管理システムは、汎用のパーソナルコンピュータ等のデータ処理装置１００と、このデータ処理装置１００に例えばＬＡＮ（Local Area Network）等の有線ネットワークもしくは無線ネットワークを介して接続されたデータ記録再生装置２００とから構成されている。なお、図５において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その説明は省略する。

【００８４】データ処理装置１００は、第１実施形態で上述したストレージ１０，暗号化ファイルシステム１１，ストレージ２０，ファイルシステム２１，上位ファイルシステム３０，アプリケーション実行モジュール４０，オペレーティングシステム５０，アクセス監視モジュール６０，フィルタモジュール７０，認証モジュール７１および切替モジュール７２をそなえて構成されると

ともに、さらにネットワークファイルシステム１０１をそなえている。

【００８５】ネットワークファイルシステム１０１は、外部の有線ネットワークもしくは無線ネットワークとのインタフェース機能を果たし、且つ、データ記録再生装置２００における暗号機能なしのストレージ（蓄積媒体）を管理するものである。また、データ記録再生装置２００は、フィルタモジュール７０によって暗号化されたコンテンツ（著作物ファイル／著作物データ）を蓄積する第２蓄積装置として機能し、暗号機能なしのストレージ２０と同様の機能を果たすものである。このデータ記録再生装置２００におけるストレージには、データ処理装置１００側からは、ネットワークファイルシステム１０１を介してアクセスされる。ただし、データ記録再生装置２００におけるストレージから読み出されたデータは、ネットワークを介してデータ処理装置１００で受け取られるまで、暗号化されたままである。なお、処理手順については第１実施形態と同様であるので、その説明は省略する。

【００８６】このように、本発明の第２実施形態としてのデータ管理システムによれば、第１実施形態と同様の作用効果が得られるほか、ユーザが誤ってネットワーク経由でデータ複製を行なったとしても、著作権を侵害することがない。

【００８７】〔３〕第３実施形態の説明

図６は本発明の第３実施形態としてのデータ管理システムの構成を示すブロック図、図７は第３実施形態のデータ管理システムにおける排他制御手法について説明するための図である。図６に示すように、第３実施形態のデータ管理システムも第１実施形態のものと同様に構成されているが、第３実施形態のデータ管理システムは、汎用のパーソナルコンピュータ等のデータ処理装置１００と、このデータ処理装置１００に外付けされたハードディスクレコーダ等のデータ記録再生装置３００とから構成されている。なお、図６や図７において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その説明は省略する。

【００８８】第３実施形態のデータ処理装置１００には、第１実施形態で上述した暗号化ファイルシステム１１，ストレージ２０，ファイルシステム２１，上位ファイルシステム３０，アプリケーション実行モジュール４０，オペレーティングシステム５０，アクセス監視モジュール６０，フィルタモジュール７０，認証モジュール７１および切替モジュール７２がそなえられており、ストレージ１０は、外付けのデータ記録再生装置３００に含まれている。つまり、第３実施形態では、データ記録再生装置３００が、暗号化ファイルシステム１１，３０１で管理される論理ドライブを含む第１蓄積装置として機能する。

【００８９】なお、データ記録再生装置３００には、ストレージ１０を管理する暗号化ファイルシステム３０１もそなえられている。そして、図７に示すごとく、第３実施形態のデータ記録再生装置３００においてもアプリケーションが動作し、このアプリケーションが、暗号化ファイルシステムストレージ１０に蓄積された著作物ファイルに対するファイルアクセスを行なうようになっている。

【００９０】データ処理装置１００とデータ記録再生装置３００とは、ＵＳＢ（UniversalSerial Bus），ＳＣＳＩ（Small Computer System Interface），ＩＥＥＥ（Institute of Electrical and Electronics Engineers）1394などの外部インタフェースを介して接続される。そして、データ処理装置１００は、データ記録再生装置３００側のストレージ１０を排他制御しながら、このストレージ１０にアクセスする。

【００９１】上述した第２実施形態では、データ処理装置１００がネットワークファイルシステム１０１を介してデータ記録再生装置２００のストレージにアクセスするので、データ記録再生装置２００がファイルアクセスのサービスを提供するのに対して、第３実施形態では、データ処理装置１００側の暗号化ファイルシステム１１が、直接、データ記録再生装置３００のストレージ１０にアクセスする点で異なっている。なお、処理手順については第１実施形態と同様であるので、その説明は省略する。

【００９２】第３実施形態では、データ記録再生装置３００におけるストレージ１０に対しては、このデータ記録再生装置３００内のアプリケーションとデータ処理装置１００側のアプリケーションとの両方からアクセスが行なわれることになるため、排他制御を行なう必要がある。ここで、図７を参照しながら、第３実施形態のデータ管理システムにおける排他制御手法について説明する。なお、図７においては、第３実施形態のデータ管理システムの要部のみが図示されている。

【００９３】図７に示すように、データ処理装置１００側には制御モジュール１０２がそなえられるとともに、データ記録再生装置３００側には制御モジュール３０２がそなえられており、これらの制御モジュール１０２と３０２とが上述した外部インタレースを介して接続され、排他制御を行なうための制御情報（排他制御信号）が、データ処理装置１００とデータ記録再生装置３００との間でやり取りされるようになっている。

【００９４】また、図７に示すように、データ処理装置１００とデータ記録再生装置３００との間では、制御情報をやり取りするための系統以外に、上述した外部インタフェースを介し、ストレージアクセスについての情報（暗号文リード／暗号文ライト）をやり取りするための系統もそなえられている。このとき、ストレージアクセスのための全ての権利を排他制御しても良く、ライトアクセスのみの権利を排他制御しても良い。

【００９５】前者の排他制御手法では、データ処理装置１００とデータ記録再生装置３００とのうちのいずれか一方がストレージ１０にアクセスしている間は、他方からのアクセスが禁止される。後者の排他制御手法では、データ処理装置１００とデータ記録再生装置３００とのうちのいずれか一方がライトアクセスしている間は、他方はリードアクセスのみが許可されライトアクセスは待たされる。リードアクセスを行なう権利は双方が有している。ただし、いずれもアクセス権を渡す場合には、暗号化ファイルシステム１１，３０１などが持つキャッシュの内容を全てフラッシュしてストレージ１０に書込みまなければならない。また、アクセス権を受け取った後については、少なくとも書き込み前に暗号化ファイルシステム１１，３０１の管理情報を再読み込みしなければならない。

【００９６】このように、本発明の第３実施形態としてのデータ管理システムによれば、第１や第２実施形態と同様の作用効果が得られる。

〔４〕その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。例えば、本実施形態の認証モジュール７１では、パスワードによる本人認証を行なっているが、本発明はこれに限定されるものではなく、指紋，声紋，虹彩，掌形等のバイオメトリクス情報を用いて本人認証を行なってもよい。

【００９７】〔５〕付記

（付記１）　コンテンツを蓄積する蓄積媒体と、該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ管理システム。

【００９８】（付記２）　該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いることを特徴とする、付記１記載のデータ管理システム。

【００９９】（付記３）　該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視することを特徴とする、付記１または付記２に記載のデータ管理システム。

（付記４）　該アプリケーション実行手段が該アプリケーションの実行を終了した場合、該アクセス監視手段が、該アプリケーションについての固有情報とこれに対応する該コンテンツについての固有情報とを該管理テーブルから削除することを特徴とする、付記３記載のデータ管理システム。

【０１００】（付記５）　該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、付記３または付記４に記載のデータ管理システム。

【０１０１】（付記６）　該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムのうちの少なくとも一つが、そのファイルシステムの全体を暗号化した上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、付記３または付記４に記載のデータ管理システム。

【０１０２】（付記７）　該暗号化ファイルシステムで管理される該論理ドライブに蓄積された該コンテンツを該アプリケーションが読み出す際に、該アクセス監視手段が、該コンテンツについての固有情報として、該アプリケーションが読み出した該コンテンツを含むファイルのファイル名を該管理テーブルに登録することを特徴とする、付記５または付記６に記載のデータ管理システム。

【０１０３】（付記８）　該暗号化ファイルシステムで管理される該論理ドライブに蓄積された該コンテンツを該アプリケーションが読み出す際に、該アクセス監視手段が、該コンテンツについての固有情報として、該アプリケーションが読み出した該コンテンツを含む論理ドライブのドライブ名を該管理テーブルに登録することを特徴とする、付記５または付記６に記載のデータ管理システム。

【０１０４】（付記９）　該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴っ

て新たに生成されたファイルのファイル名を、該アプリケーションについての固有情報に対応させて、該管理テーブルに登録することを特徴とする、付記５～付記８のいずれか一つに記載のデータ管理システム。

（付記１０）　該アクセス監視手段が、該新たに生成されたファイルのファイル名の一部もしくは全部を変更したものを該管理テーブルに登録することを特徴とする、付記９記載のデータ管理システム。

【０１０５】（付記１１）　該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その比較結果が不一致である場合、該管理テーブルに登録された該ドライブ名の論理ドライブに該新たに生成されたファイルが蓄積されるように該ファイル名を変更して該管理テーブルに登録することを特徴とする、付記８記載のデータ管理システム。

【０１０６】（付記１２）　該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その上記比較結果が一致した場合、該アクセス監視手段が、該新たに生成されたファイルのファイル名の、該管理テーブルへの登録を禁止することを特徴とする、付記８記載のデータ管理システム。

【０１０７】（付記１３）　該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その比較結果が不一致である場合、該フィルタリング手段の動作が有効化されることを特徴とする、付記８記載のデータ管理システム。

【０１０８】（付記１４）　該蓄積媒体が、電源断に伴って蓄積データを消去される一次記憶手段を含み、該フィルタリング手段が、暗号化した該新たに生成されたファイルを、該蓄積先論理ドライブに代えて該一次記憶手段に蓄積することを特徴とする、付記１３記載のデータ管理システム。

【０１０９】（付記１５）　該蓄積媒体が、該暗号化ファイルシステムで管理される該論理ドライブを含む第１蓄積装置と、該フィルタリング手段によって暗号化された該コンテンツを蓄積する第２蓄積装置とを含んで構成されていることを特徴とする、付記５～付記１４のいずれか一つに記載のデータ管理システム。

【０１１０】（付記１６）　該アプリケーション実行手段，該アクセス監視手段，該フィルタリング手段および該第１蓄積装置が、一つのデータ処理装置内にそなえられるとともに、該第２蓄積装置が、ネットワークを介して該データ処理装置に接続されていることを特徴とする、付記１５記載のデータ管理システム。

【０１１１】（付記１７）　ユーザの本人認証を行なうための認証手段と、該認証手段によって該ユーザの本人認証が行なわれた場合にのみ該フィルタリング手段の動作の有効化／無効化を切り替える切替手段とをさらにそなえたことを特徴とする、付記１～付記１６のいずれか一つに記載のデータ管理システム。

【０１１２】（付記１８）　該アプリケーション実行手段，該アクセス監視手段，該フィルタリング手段および該第２蓄積装置が、一つのデータ処理装置内にそなえられるとともに、該第１蓄積装置が、該データ処理装置に外付けされるデータ記録再生装置に含まれていることを特徴とする、付記１６記載のデータ管理システム。

【０１１３】（付記１９）　蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ処理装置。

【０１１４】（付記２０）　蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションが動作している際に、該コンテンツの著作権を保護する機能をコンピュータによって実現させるためのデータ管理プログラムであって、動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段、および、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段として、コンピュータを機能させることを特徴とする、データ管理プログラム。

【０１１５】（付記２１）　蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションが動作している際に、該コンテンツの著作権を保護する機能をコンピュータによって実現させ

るためのデータ管理プログラムを記録したコンピュータ読取可能な記録媒体であって、該データ管理プログラムが、動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段、および、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段として、該コンピュータを機能させることを特徴とする、データ管理プログラムを記録したコンピュータ読取可能な記録媒体。

【０１１６】

【発明の効果】以上詳述したように、本発明（請求項１～５）によれば、蓄積媒体に蓄積されたコンテンツがアプリケーションによってアクセスされると、そのアクセス状況がアプリケーション毎に管理され、アプリケーションによって読み出されて利用されているコンテンツは、そのアプリケーションについての固有情報を用いて暗号化／復号化される。

【０１１７】これにより、暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況下において、アプリケーションが、暗号機能ありの蓄積媒体に蓄積された暗号化コンテンツを読み出し、そのコンテンツを暗号化機能なしの蓄積媒体に一時的に格納しながら利用したとしても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護することができ、データ管理システムの性能向上に寄与するところが大きい。

【０１１８】つまり、ディジタル化された著作物データ（ディジタルコンテンツ）が暗号化された上で蓄積されるので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意に蓄積媒体のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【０１１９】このとき、アプリケーションについての固有情報として、オペレーティングシステムによって与えられるプロセス毎の識別情報（プロセスＩＤ）のような動的な情報を用い、その識別情報でコンテンツの暗号化を行なうことにより、同じアプリケーションであっても起動時期が異なると復号化することができず、蓄積媒体上のファイルを通して復号化されたデータが容易に交換されなくなるので、著作権の侵害をより確実に防ぐことができる。

【０１２０】また、ユーザの本人認証が行なわれた場合にのみフィルタリング手段の動作の有効化／無効化を切り替えるように構成することにより、著作者自身や著作者の許諾を得た者（例えば著作物を編集するなど二次著作物を生成する者）を登録しておけば、著作者自身や著作者の許諾を得た者は、フィルタリング手段の動作を無効化することができ、作業を不当に制限されず、著作権の行使の著しい制限に伴う著作権侵害の発生を防止することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態としてのデータ管理システムの構成を示すブロック図である。

【図２】第１実施形態のデータ管理システムにおけるアクセス監視モジュールの処理手順を説明するためのフローチャートである。

【図３】第１実施形態のデータ管理システムにおけるフィルタモジュールの処理手順を説明するためのフローチャートである。

【図４】第１実施形態のデータ管理システムの変形例の構成を示すブロック図である。

【図５】本発明の第２実施形態としてのデータ管理システムの構成を示すブロック図である。

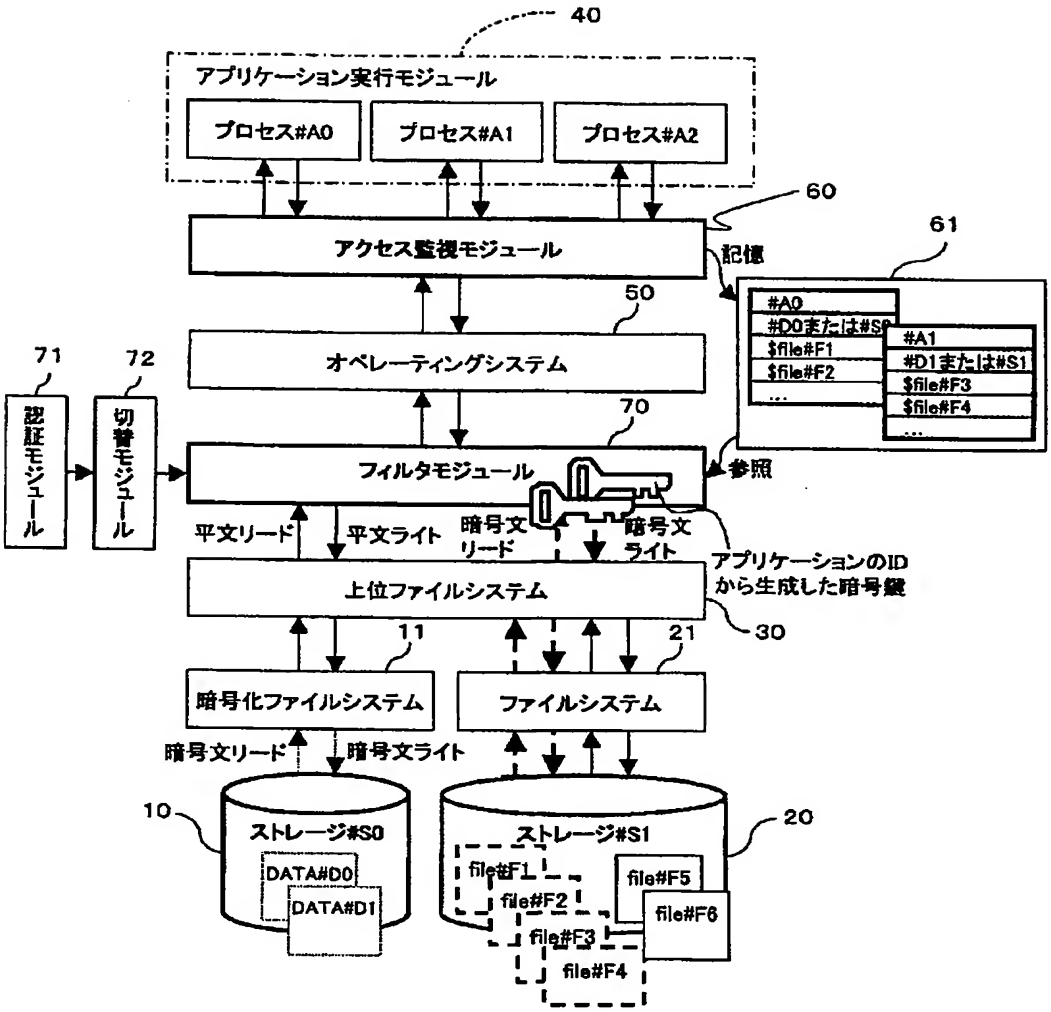
【図６】本発明の第３実施形態としてのデータ管理システムの構成を示すブロック図である。

【図７】第３実施形態のデータ管理システムにおける排他制御手法について説明するための図である。

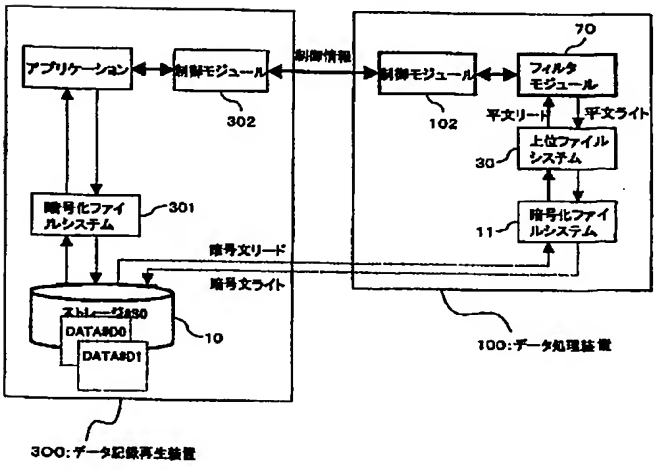
【符号の説明】

１０　ストレージ（暗号化機能ありの蓄積媒体，第１蓄積装置）
１１　暗号化ファイルシステム
２０　ストレージ（暗号化機能なしの蓄積媒体，第２蓄積装置）
２１　ファイルシステム（ＦＡＴ）
３０　上位ファイルシステム
４０　アプリケーション実行モジュール（アプリケーション実行手段）
５０　オペレーティングシステム
６０　アクセス監視モジュール（アクセス監視手段）
６１　管理テーブル（リスト）
７０　フィルタモジュール（フィルタリング手段）
７１　認証モジュール（認証手段）
７２　切替モジュール（切替手段）
８０　ストレージ（蓄積媒体）
１００　データ処理装置
１０１　ネットワークファイルシステム
１０２　制御モジュール
２００　データ記録再生装置（第２蓄積装置）
３００　データ記録再生装置（第１蓄積装置）
３０１　暗号化ファイルシステム
３０２　制御モジュール

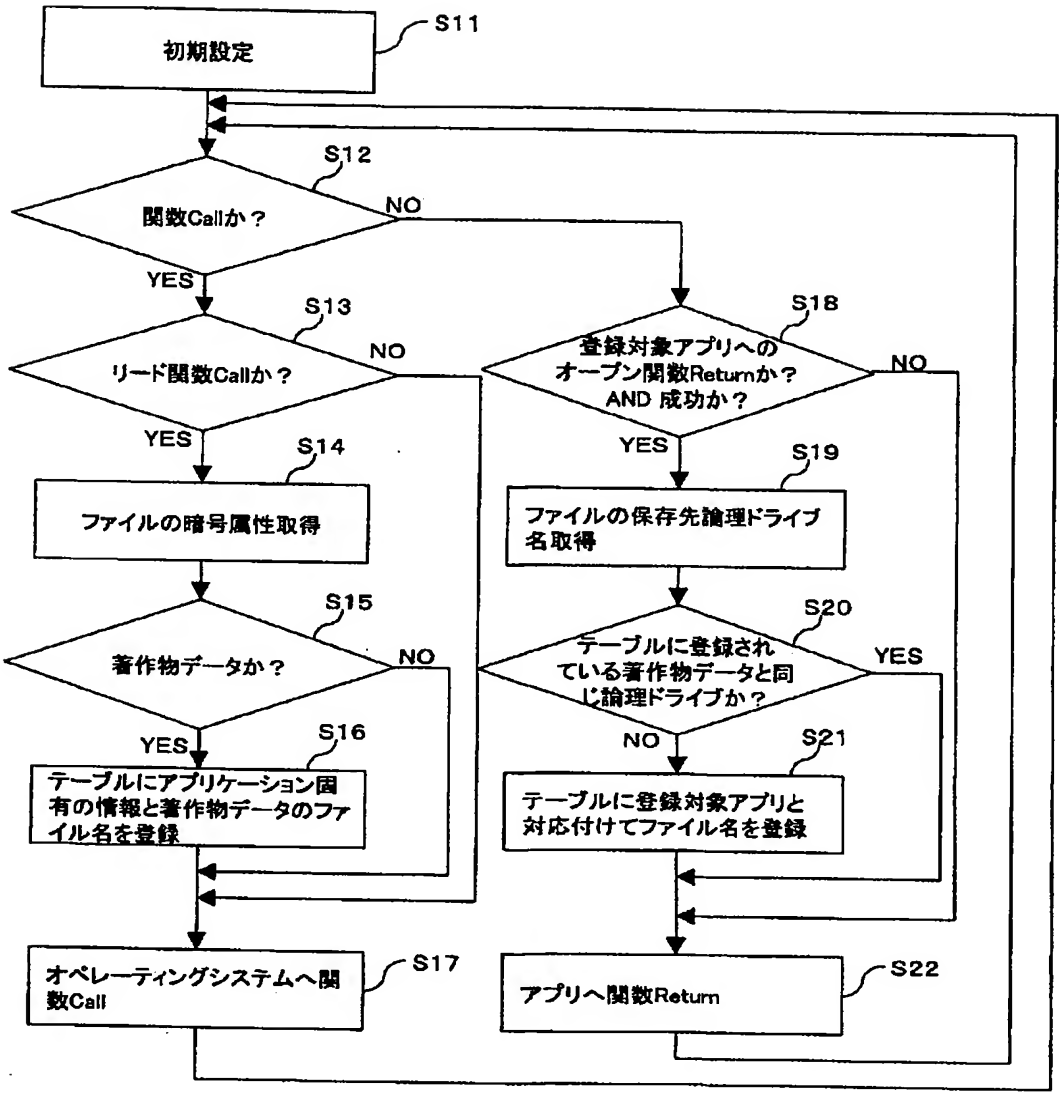
【図１】


40
アプリケーション実行モジュール
プロセス#A0
プロセス#A1
プロセス#A2
60
アクセス監視モジュール
記憶
61
#A0
#D0または#S0
$file#F1
$file#F2
...
#A1
#D1または#S1
$file#F3
$file#F4
...
50
オペレーティングシステム
71
認証モジュール
72
切替モジュール
70
フィルタモジュール
参照
平文リード
平文ライト
暗号文リード
暗号文ライト
アプリケーションのIDから生成した暗号鍵
上位ファイルシステム
30
11
21
暗号化ファイルシステム
ファイルシステム
暗号文リード
暗号文ライト
10
ストレージ#S0
DATA#D0
DATA#D1
20
ストレージ#S1
file#F1
file#F2
file#F3
file#F4
file#F5
file#F6

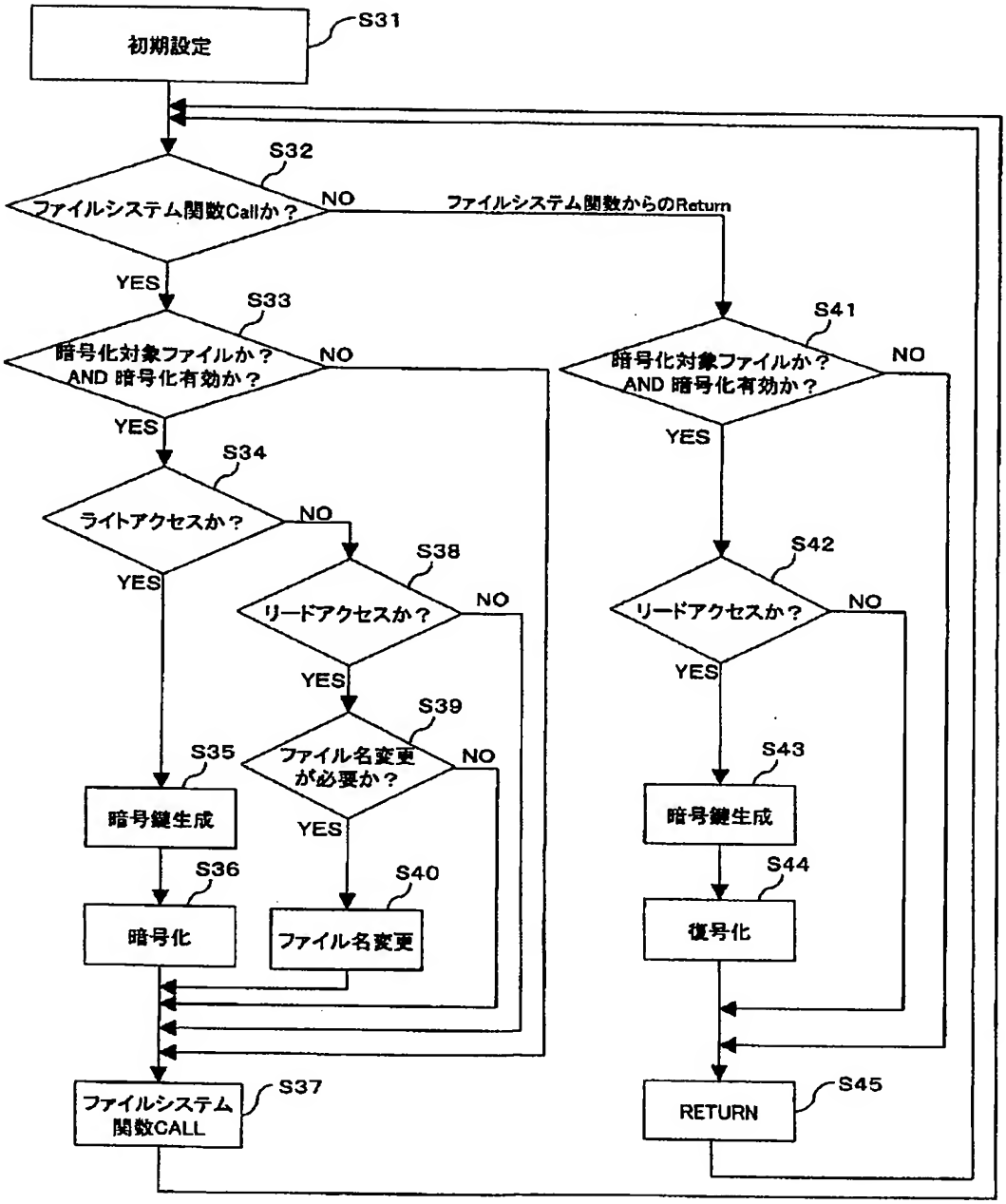
【図７】


アプリケーション
制御モジュール
302
制御情報
制御モジュール
102
フィルタモジュール
70
平文リード
平文ライト
上位ファイルシステム
30
暗号化ファイルシステム
11
301
暗号文リード
暗号文ライト
10
DATA#D0
DATA#D1
100:データ処理装置
300:データ記録再生装置

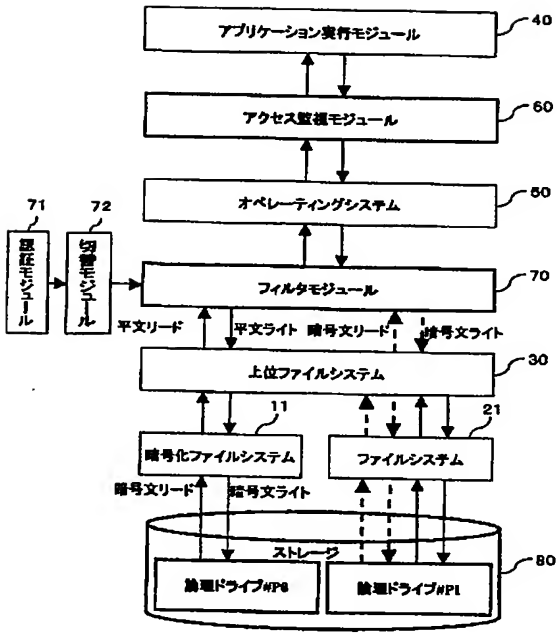
【図２】


初期設定
S11
S12
関数Callか？
NO
YES
S13
リード関数Callか？
NO
YES
S14
ファイルの暗号属性取得
S15
著作物データか？
NO
YES
S16
テーブルにアプリケーション固有の情報と著作物データのファイル名を登録
S17
オペレーティングシステムへ関数Call
S18
登録対象アプリへのオープン関数Returnか？ AND 成功か？
NO
YES
S19
ファイルの保存先論理ドライブ名取得
S20
テーブルに登録されている著作物データと同じ論理ドライブか？
YES
NO
S21
テーブルに登録対象アプリと対応付けてファイル名を登録
S22
アプリへ関数Return

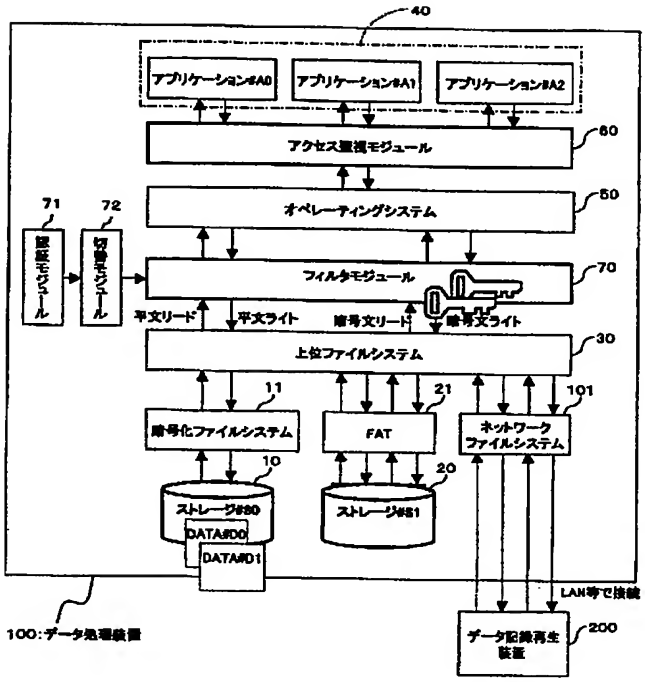
【図３】


初期設定
S31
S32
ファイルシステム関数Callか？
NO
ファイルシステム関数からのReturn
YES
S33
暗号化対象ファイルか？
AND 暗号化有効か？
NO
YES
S34
ライトアクセスか？
NO
YES
S38
リードアクセスか？
NO
YES
S39
ファイル名変更
が必要か？
NO
YES
S35
暗号鍵生成
S36
暗号化
S40
ファイル名変更
S37
ファイルシステム
関数CALL
S41
暗号化対象ファイルか？
AND 暗号化有効か？
NO
YES
S42
リードアクセスか？
NO
YES
S43
暗号鍵生成
S44
復号化
S45
RETURN

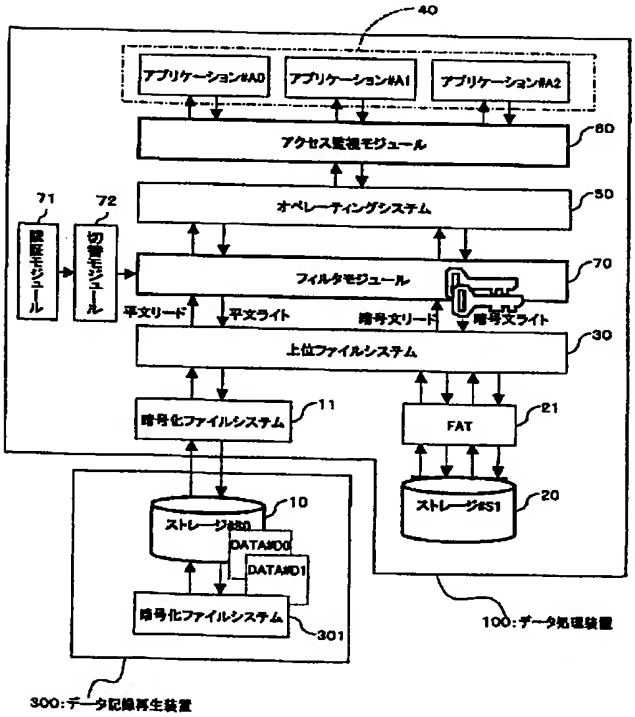
【図４】


アプリケーション実行モジュール
40
アクセス監視モジュール
60
オペレーティングシステム
50
71
72
認証モジュール
切替モジュール
フィルタモジュール
70
平文リード
平文ライト
暗号文リード
暗号文ライト
上位ファイルシステム
30
11
21
暗号化ファイルシステム
ファイルシステム
暗号文リード
暗号文ライト
ストレージ
論理ドライブ#P0
論理ドライブ#P1
80

【図５】


40
アプリケーション#A0
アプリケーション#A1
アプリケーション#A2
アクセス監視モジュール
60
オペレーティングシステム
50
71
72
認証モジュール
切替モジュール
フィルタモジュール
70
平文リード
平文ライト
暗号文リード
暗号文ライト
上位ファイルシステム
30
11
21
101
暗号化ファイルシステム
FAT
ネットワーク
ファイルシステム
10
20
ストレージ#S0
ストレージ#S1
DATA#D0
DATA#D1
LAN等で接続
100:データ処理装置
データ記録再生
装置
200

【図６】


40
アプリケーション#A0
アプリケーション#A1
アプリケーション#A2
アクセス監視モジュール
60
オペレーティングシステム
50
71
72
認証モジュール
切替モジュール
フィルタモジュール
70
平文リード
平文ライト
暗号文リード
暗号文ライト
上位ファイルシステム
30
暗号化ファイルシステム
11
FAT
21
ストレージ#S0
ストレージ#S1
10
20
DATA#D0
DATA#D1
暗号化ファイルシステム
301
100:データ処理装置
300:データ記録再生装置

フロントページの続き

Ｆターム（参考）　5B017 AA03 AA06 BA07 BA09 CA07
　　CA16
　　5B082 EA11 GA00
　　5J104 AA01 PA14